



מחברת בחינה

לאחר סיום כתיבת הבדיקה יש למסור את המחברת למושגין ולזובג בשקט את חדר הבדיקה.
אין להכניס לחדר הבדיקה חומר עזר — ספרים, חברים, רשיומות — חוץ מ"חומר עזר מותר בשימוש" המפורט בגוף השאלון או בהוראות מוקדמות של המשרד. כמו כן אין להכניס לחדר הבדיקה טלפונים או מכשירים אלקטרוניים אחרים. שימוש בחומר עזר שאינו מותר יוביל לפסילת הבדיקה.
הבדיקה נועדה לבדוק הישגים אישיים, וכך יש לעבוד בעבודה עצמית בלבד. בזמן הבדיקה אין להיעזר בזולות ואין לתת או לקבל חומר בכתב או בעל פה.

יש לקרוא את ההוראות בעמוד זה ולמלא אותו בדיקנות. אידמיות ההוראות עלול לגרום לתקלות ואף להביא לידי פסילת הבדיקה.

לנבחנים ולנבחנות שלום,

יש להקפיד על טוהר הבדיקות !

הוראות לבחינה

1. יש לוודא כי בבדיקה הנבחן שקיבלת מודפסים הפרטים האישיים האישיים שלך. אין להוסיף או לשנות שם פרט בבדיקות, כדי למנוע עיכוב בזיהוי המחברת ובירושים הציוניים.
 2. אם לא קיבלת מדבכה, יש למלא בכתב יד את הפרטים במקום המיועד לבדיקה הנבחן.
 3. אסור לכתוב בשולי המחברת (החלק המקורי) משום שחלק זה לא ייסרק.
 4. לטיווח ישמשו ארך ורקע מחברת הבדיקה שייעודו לך.
 5. אין לתולש או להוסיף דפים. מחברת שתזוגש לא שלמה תעורר חשד לאי-קיים טוהר הבדיקות.
 6. אין לכתוב שם בתור המחברת משום שהביקורת נבדקת בעילום שם.

ב ה אלמה!

אם ויחוה מחרברת נוספת

إذاً أُعطي دفتر إضافيٌ

* التعليمات باللغة العربية علم ظهر الصفحة

A small, empty rectangular box with a thin black border, likely intended for a student to draw or write something.

יש לסייע רשות

يجب الإشارة في المرّبع

دفتر امتحان

تحية للمتحدين وللمتحنات ،

يجب قراءة التعليمات في هذه الصفحة والعمل وفقاً لها بدقة . عدم تنفيذ التعليمات قد يؤدي إلى عوائق مختلفة وحتى إلى إلغاء الامتحان .
 أعد الامتحان لفحص التحصيلات الشخصية، لذلك يجب العمل بشكل ذاتي فقط . أثناء الامتحان، لا يسمح طلب المساعدة من الغير، ولا يسمح إعطاء أو الحصول على مواد مكتوبة أو شفهية .
 لا يسمح إدخال مواد مساعدة – كتب، دفاتر، قوائم – إلى غرفة الامتحان، ما عدا "مواد مساعدة يسمح استعمالها" المفصلة في نموذج الامتحان أو في تعليمات مسابقة من وزارة التربية والتعليم . كما لا يسمح إدخال هواتف خلوية أو أجهزة إلكترونية أخرى إلى غرفة الامتحان . استعمال مواد مساعدة لا يسمح استعمالها سوف يؤدي إلى إلغاء الامتحان .
 بعد الانتهاء من كتابة الامتحان، يجب تسليم الدفتر للمراقب ومجادرة غرفة الامتحان بهدوء .

يجب التّقييد بنزاهة الامتحانات !

تعليمات لامتحان

1. يجب التأكيد بأن تفاصيلك الشخصية مطبوعة على ملصقات الممتحن التي حصلت عليها . لا يسمح بإضافة أو تغيير أي تفاصيل في الملصقات، وذلك لمنع عوائق في تشخيص الدفتر وفي تسجيل العلامات .
2. في حال عدم حصولك على ملصقة، يجب ملء التفاصيل في المكان المعد لملصقة الممتحن، بخط يد .
3. لا يسمح الكتابة في هوماش الدفتر (في المنطقة المخططة)، لأنه لن يتم مسح ضوئي لهذه المنطقة .
4. للمسؤولة تُستعمل أوراق دفتر الامتحان المعدة لذلك فقط .
5. يُمنع نزع أو إضافة أوراق . الدفتر الذي يسلم ناقصاً يُشير الشك بعدم الالتزام بنزاهة الامتحانات .
6. لا يسمح كتابة الاسم داخل الدفتر، لأن الامتحان يُفحص بدون ذكر اسم .

نتمي لكم النجاح!



סוג הבדיקה: גמר לבתי-ספר לטכניים ולהנדסאים

מועד הבדיקה: אביב תשפ"ב, 2022

שם השאלון: 735913

מספר: מילון מונחים

מדינת ישראל

משרד החינוך

יישומי ניתוב IP וابتחה ברשותות קmphos

הוראות לנבחנים

א. **משך הבדיקה:** ארבע שעות.

ב. **מבנה השאלון ופתחה הערכתי:** בשאלון זה שני פרקים:

פרק ראשון: יישומי ניתוב IP	45	נקודות
פרק שני: אבטחה ברשותות Kmpos	55	נקודות
סך-הcool	100	נקודות

בשאלון זה שיש שאלות. יש לענות על השאלות על-פי ההוראות שבסל פרק.

ג. **חומר עזר מותר בשימוש:** כל חומר עזר כתוב בכתב-יד או מודפס על נייר.

ד. **הוראות מיוחדות:**

1. כתבו את כל התשובות בגוף השאלון, במקום המועד לכך.

2. **כתבו בעט בלבד.**

3. עמודים 25–27 משמשים כתיווחה.

4. הדבקו את מדבקות הנבחן במקומות המועדים לכך.

5. בנספח לשאלון זה מובא מילון מונחים בשפות עברית, ערבית, אנגלית ורוסית. תוכלו להיעזר בו בעת הצורך.

בשאלון זה **28 עמודים ו-2 עמודי נספח.**

בהצלחה!

◀ המשך מעבר לדף ◀

השאלות

בשalon זה, כתבו את התשובות במקומות המועד לכך.
בשאלות רב-ברירה, לכל שאלה ארבע תשובות, אך רק אחת מהן נכונה. הקיפו בעיגול את הספרה המציינת את התשובה הנכונה.
בשאלות האחרות, פעלו על-פי ההנחיות.

פרק ראשון: ישומי ניתוב IP (45 נקודות)

ענו על כל השאלות 1–3, על-פי ההנחיות (לכל שאלה – 15 נקודות).

שאלה 1 (15 נקודות)

ענו על חמשה מבין הסעיפים א'–ו' על-פי ההנחיות שבכל סעיף (לכל סעיף – 3 נק').

א. הוגדר איזור OSPF המכיל את הרשאות אלה:

164.165.8.0

164.165.10.0

164.165.12.0

164.165.14.0

סכמו את הנתיבים הללו בצורה ידנית (route summarization) לכדי נתיב אחד.

תשובה:

Net id: _____

Subnet mask: _____

ב. איזה מהබאים **אינו** סוג של הודעה של פרוטוקול הניתוב BGP ?(BGP message type)

open .1

update .2

ack .3

keepalive .4



735913 يـسـوـمـيـ نـيـتوـبـ IP وـأـبـطـاـهـ بـرـشـتـوـتـ كـمـفـوسـ، أـبـيـبـ تـشـفـ"ـبـ، سـمـلـ 3ـ

- ג. מה יעשה פרוטוקול הניתוב EIGRP אם ה-successor route נפל, ולא קיים ?feasible successor?
1. יגדיר את הנתיב כ-passive עד שיימצא successor חדש
 2. ישלח בקשות query לנטים השכנים עד שיימצא successor חדש
 3. יעביר תעבורת לנット השכן עם ה-administrative distance הנמוך ביותר
 4. יפיק מחדש נתיבים של פרוטוקול הניתוב OSPF
- ד. איזו פקודה ב-IOS CISCO מאפשרת סיקום אוטומטי של רשתות?
- תשובה:

R1(config-router)# _____

- ה. באיזה TCP Port משתמש פרוטוקול הניתוב BGP כדי להחליף הודעות בין נתבים?
- תשובה: _____
- ו. קבעו לגבי כל אחד מן ההיגדים שלහן אם הוא **נכון** או **לא נכון**, והקיימו בעיגול את התשובה הנכונה.
1. ה-weight attribute בפרוטוקול הניתוב BGP הוא קנייני של חברת סיסקו. **נכון / לא נכון**
 2. ה-weight attribute בפרוטוקול הניתוב BGP הוא הקритריון הראשון שנבדק בתהליך בחירת הנתיב הטוב ביותר אל היעד בנתבי סיסקו. **נכון / לא נכון**



ישומי ניתוב IP ואמתכה ברשותת קמפוס, אביב תשפ"ב, סמל 735913

שאלה 2 (15 נקודות)

ענו על חמשה מ בין הסעיפים א'-ו' על-פי ההנחיות שבכל סעיף (לכל סעיף – 3 נקודות).

א. התבוננו בפלט שלහן:

R1

interface Loopback0

ip address 172.16.1.33 255.255.255.224

interface FastEthernet0/0

ip address 192.168.12.1 255.255.255.0

router BGP 100

neighbor 192.168.12.2 remote-as 100

על-פי הפלט, מהי הפקודה שיש להגדיר בנתב R1 כדי שנתב זה יפרסם את Loopback0 ב프וטוקול הניתוב ?BGP

network 172.16.1.32 mask 255.255.255.224 .1

network 172.16.1.0 0.0.0.255 .2

network 172.16.1.32 255.255.255.224 .3

network 172.16.1.32 mask 0.0.0.31 .4

ב. ב프וטוקול הניתוב OSPF, איזו כתובת multicast משמשת לשילוח ?(Designated Router)

224.0.0.5 .1

224.0.0.1 .2

224.0.0.6 .3

224.0.0.2 .4

735913 יישומי ניתוב IP ו Abedha برشتوت كمفووس، ابب تشـ"ب، سـمـلـ 735913

٦. سييمتم لهجيـر اـت فـروـتـوكـولـ النـيـتـوبـ OSPFـ بـفـرـوـيـكـتـ شـعـبـدـتـمـ عـلـيـوـ. لـاـخـرـ بـدـيـكـهـ شـلـ الـهـجـدـرـوـتـ غـلـيـتـمـ
ـقـيـ شـحـثـمـ لـهـجـيـرـ Router-IDـ بـنـتـبـ R1ـ.

لهـلـنـ فـلـطـ شـلـ مـمـشـكـيـ النـتـبـ R1ـ:

Interface	IP-Address	OK? Method Status	Protocol
GigabitEthernet0/0	192.168.1.1	YES manual up	up
GigabitEthernet0/1	192.168.2.1	YES manual up	up
GigabitEthernet0/2	unassigned	YES unset administratively down down	
Serial0/3/0	192.168.23.1	YES manual up	up
Serial0/3/1	unassigned	YES unset administratively down down	
Vlan1	unassigned	YES unset administratively down down	

איـزوـ مـبـينـ الـكتـوبـوـتـ الـمـوـفـعـوـتـ بـفـلـطـ هـذـهـ نـبـرـهـاـ C~ID~ Router~?

تـشـوـبـهـ:

٧. باـيـهـ سـوـجـدـرـ شـمـوـجـدـرـ بـوـ فـرـوـتـوكـولـ OSPFـ نـيـتـنـ لـعـشـوـتـ سـيـقـومـ نـتـيـبـيـمـ (route summarization)

- Backbone Router .1
- ABR (Area Border Router) .2
- DR (Designated Router) .3
- על כל נתב המוגדר עם פרוטוקול OSPF .4



ישומי ניתוב IP ואבטחה ברשות Kmpos, אביב תשפ"ב, סמל 735913

- ה. בנתב R1 הוגדר פרוטוקול הניתוב OSPF. מנהל הרשות החליט לשנות את ה-id-router באמצעות ההגדירות
האלה:

```
R1(config)# router ospf 100
```

```
R1(config-router)# router-id 1.1.1.1
```

```
R1(config-router)# exit
```

לאחר כתיבת ההגדירות, כתב מנהל הרשות בנתב R1 את הפקודה: show ip protocols, וקיבל את הפלט זהה:

```
R1#show ip protocols
```

Routing Protocol is "ospf 1"

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Router ID 200.0.0.0

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Maximum path: 4

Routing for Networks:

192.168.7.0 0.0.0.255 area 0

192.168.8.0 0.0.0.255 area 0

192.168.9.0 0.0.0.255 area 0

192.168.10.0 0.0.0.255 area 0

192.168.11.0 0.0.0.255 area 0

192.168.12.0 0.0.0.255 area 0

200.0.0.0 0.0.0.255 area 0

Routing Information Sources:

Gateway	Distance	Last Update
1.1.1.1	110	00:00:18
2.2.2.2	110	00:01:13
3.3.3.3	110	00:00:18
200.0.0.0	110	00:00:18

Gateway	Distance	Last Update
1.1.1.1	110	00:00:18
2.2.2.2	110	00:01:13
3.3.3.3	110	00:00:18
200.0.0.0	110	00:00:18

Gateway	Distance	Last Update
1.1.1.1	110	00:00:18
2.2.2.2	110	00:01:13
3.3.3.3	110	00:00:18
200.0.0.0	110	00:00:18

Gateway	Distance	Last Update
1.1.1.1	110	00:00:18
2.2.2.2	110	00:01:13
3.3.3.3	110	00:00:18
200.0.0.0	110	00:00:18

Gateway	Distance	Last Update
1.1.1.1	110	00:00:18
2.2.2.2	110	00:01:13
3.3.3.3	110	00:00:18
200.0.0.0	110	00:00:18

Gateway	Distance	Last Update
1.1.1.1	110	00:00:18
2.2.2.2	110	00:01:13
3.3.3.3	110	00:00:18
200.0.0.0	110	00:00:18

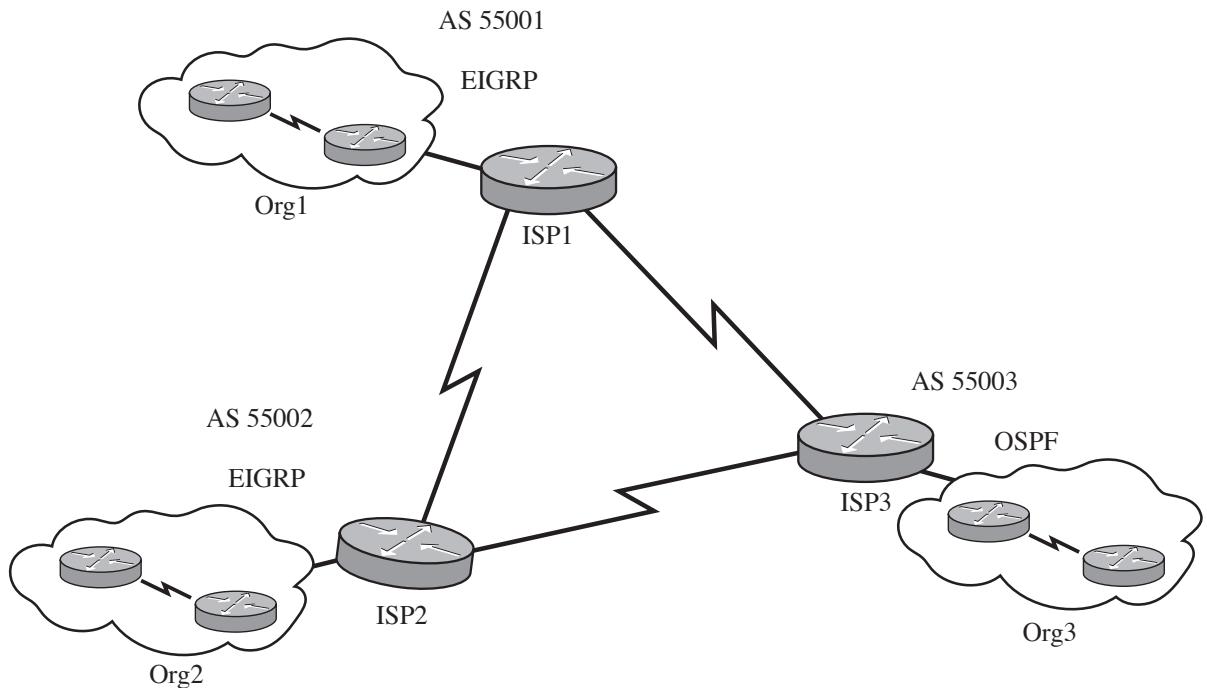
Gateway	Distance	Last Update
1.1.1.1	110	00:00:18
2.2.2.2	110	00:01:13
3.3.3.3	110	00:00:18
200.0.0.0	110	00:00:18

איו פולה יש לנוקוט כדי לתקן את הבעיה?

1. להפעיל את הפקודה: reload ospf
2. לשמר את ההגדירות באמצעות הפקודה: copy running-config startup-config
3. לשנות את כתובות ה-id-router לכתוות אחרת
4. לבצע אתחול לפרטוקול הניתוב OSPF באמצעות הפקודה: clear ip ospf process

יישומי ניתוב IP ובטוחה ברשות קמפווס, אביב תשפ"ב, סמל 735913

ו. התבוננו בטופולוגיה שלහן:



באיזה פרוטוקול ניתוב משתמש כדי להעביר מידע על נתיבים בין הנטבים הנמצאים באותו מערכות?
?AS (Autonomous System)

ב- .1 default routing protocol

ב- .2 Interior Gateway Protocol (IGP) routing protocols

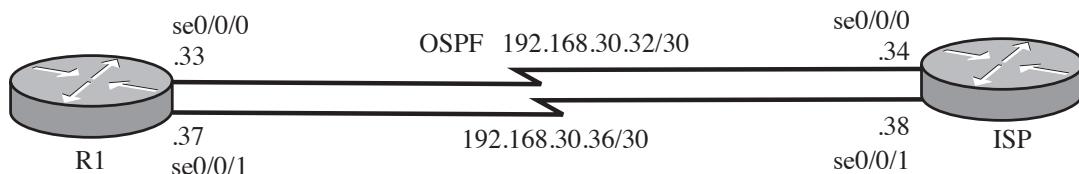
ב- .3 Exterior Gateway Protocol (EGP) routing protocols

ב- .4 static routing protocol

שאלה 3 (15 נקודות)

ענו על חמשה מבין הסעיפים א'-ו' על-פי ההנחיות שבכל סעיף (לכל סעיף – 3 נקודות).
שים לב: סעיפים ה' וו' תלויים זה זה.

א. התבוננו בטופולוגיה של להן:



באמצעות פרוטוקול הניתוב OSPF, נתב R1 יצר יחסי שכנות עם נתב ISP על-גבי רשת 192.168.30.32/30. רשת 192.168.30.36/30 מיועדת לשמש **נתיב גיבוי** בעת קriseת החיבור הקיים. לכן הוגדרה על נתב R1 הפקודה שלללה:

```
ip route 0.0.0.0 0.0.0.0 S0/0/1 100
```

מאז שהוגדרה הפקודה, תובנות הניטוב של הנתונים נועשו כולה על נתיב הגיבוי, אף על פי שהנתיב המכוון נמצא במצב UP ומתקף היטב.

איזה פועלה יש לנקוט כדי להתגבר על הבעייה?

- .1 להוציא את כתובת ה-IP של ה-next hop
 - .2 לשנות את ה-administrative distance ל-1 בנתיב הסטטי
 - .3 לשנות את ה-administrative distance ל-120 בנתיב הסטטי
 - .4 לשנות את רשות היעד ל-192.168.30.34

ב. קבעו לגבי כל אחד מן היגדים שלහן אם הוא נכון לא נכון בעיגול את התשובה הנכונה.

- פרוטוקולי הניתוב OSPF ו-EIGRP תומכים ב-**equal** load balancing.
 - פרוטוקול הניתוב EIGRP תומך ב-**unequal** load balancing.

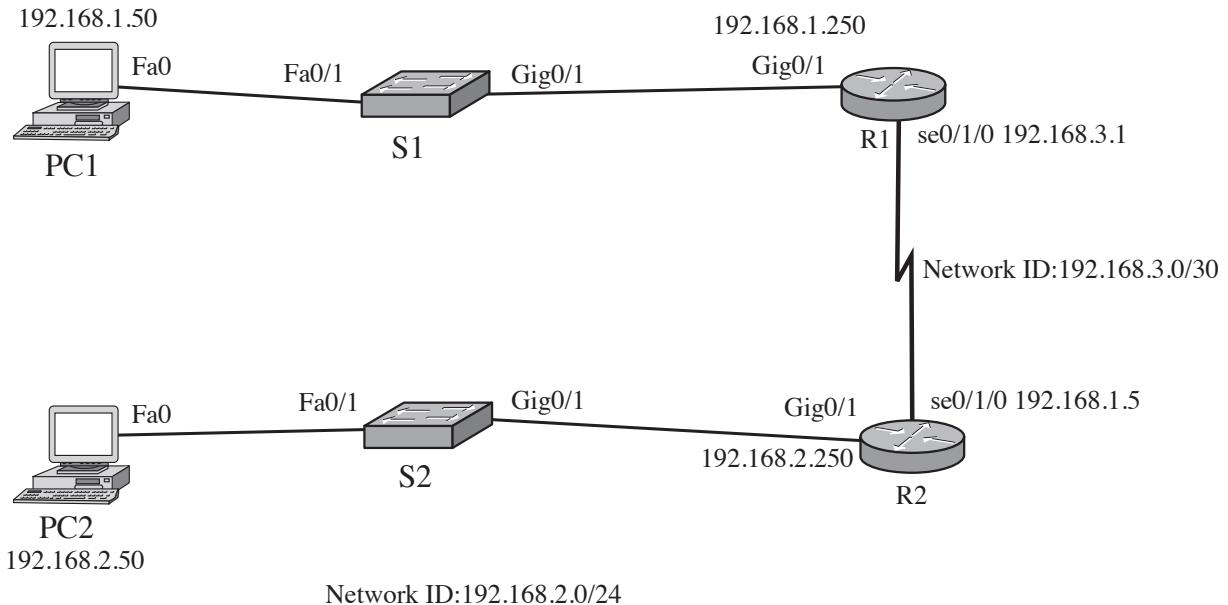
ג. למה נועדה הפקודה **IPv6 unicast-routing** בהתקני Cisco IOS ?

1. לאפשר ניתוב באמצעות IPv6
 2. לאפשר ניתוב של מנוגות unicast בנתב
 3. לשיק את הנתב לקבוצת multicast ה-*multicast* של כל הנתבים בראשת
 4. למנייעת הצטרופות הנתב לקבוצת multicast ה-*multicast* של כל הנתבים בראשת

735913 יישומי ניתוב IP ובטוחה ברשותות קמפווס, אביב תשפ"ב, סמל

- ד. התבוננו בטופולוגיה שלහן ובפלט הפקודה: `show ip protocols`

Network ID:192.168.1.0/24



```

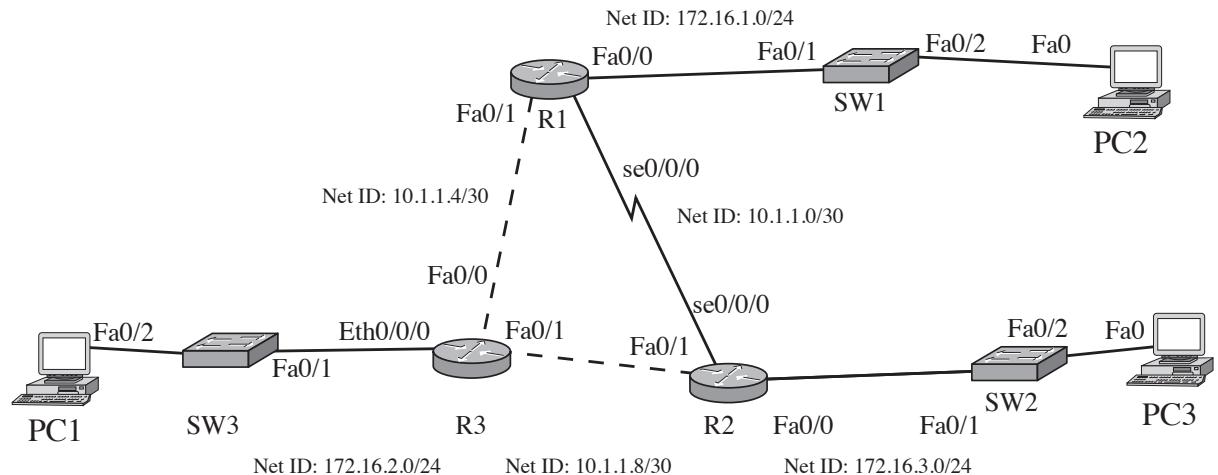
R1#show ip protocols
Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 100.100.100.100
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.3.1 0.0.0.0 area 0
    192.168.1.250 0.0.0.0 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway          Distance      Last Update
    100.100.100.100        110          00:02:29
  Distance: (default is 110)
  
```

מנהל הרשת הגדר פרוטוקול ניתוב OSPFv2 על שני נתבים של חברת סייסקו. הנתבים אינם מצליחים לבסס יחסי שכנות ביניהם. מה צריך לעשות כדי להתגבר על הבעיה?

1. יש להוסיף את הפקודה: `R1 network 192.168.0.0 0.0.255.255` לנtab R1
2. יש להסיר את הפקודה `passive gigabitEthernet0/1` מנתב R1
3. יש להוסיף את הפקודה `R1 Network 192.168.3.0 0.0.255 area 0` לנtab R1
4. יש לשנות בנתב R2 את כתובת ה-IP עבור ממשק Se0/1/0 לכתובת 192.168.3.2 את כתובת ה-IP עבור ממשק Se0/1/0 לכתובת 192.168.3.2

ישומי ניתוב IP ואבטחה ברשותם קמפוס, אביב תשפ"ב, סמל 735913

הטופולוגיה והפלטים שלהן מתייחסים לסעיפים ה'-ו', התלוים זה זה.



```
R3#show running-config | section interface
interface FastEthernet0/0
  ip address 10.1.1.5 255.255.255.252
  duplex auto
  speed auto
interface FastEthernet0/1
  ip address 10.1.1.9 255.255.255.252
  duplex auto
  speed auto
interface Ethernet0/0/0
  ip address 172.16.2.254 255.255.255.0
  duplex auto
  speed auto
```

```
R3#show running-config | section router
router eigrp 100
  passive-interface FastEthernet0/0
  passive-interface FastEthernet0/1
  passive-interface Ethernet0/0/0
  network 172.16.2.0 0.0.0.255
  network 10.1.1.4 0.0.0.3
  network 10.1.1.8 0.0.0.3
  no auto-summary
```

735913 יישומי ניתוב IP ובטחה ברשותה למפוס, אביב תשפ"ב, סמל

ה. בהנחה שהנתבים R1 ו-R2 מוגדרים נכון, מה הסיבה שבגללה נתב R3 אינוצליח לבסס יחס שכנות עם נתבים R1 ו-R2?

1. לא הוגדרה פקודת `Network` עבור רשת 10.1.1.0/24 בנתב R3

2. כל משקי נתב R3 מוגדרים כ-`passive interface` עבור פרוטוקול הניתוב EIGRP

3. כתובת ה-IP המוגדרת עבור משק Fa0/0 אינה נכון

4. בנתב R1 לא אפשר סיכון נתיבים אוטומטי

5. איזו פקודה צריך מנהל הרשות לכתוב כדי שנתב R3 יוכל לבסס יחס שכנות עם נתבים R1 ו-R2?

תשובה:

**פרק שני: בטיחה ברשות Kmpos (55 נקודות)****ענו על כל השאלות 4 – 6 על-פי ההנחיות שבכל שאלה.****שאלה 4 (15 נקודות)****ענו על חמשה מבין הסעיפים א' – ז' על-פי ההנחיות שבכל סעיף (לכל סעיף – 3 נקודות).**

א. איזה מגנון בטיחה יכול להתריע על מתקפה מסווג **port scanning attack** על הרשת הארגונית?

- | | |
|----------------------------------|----|
| firewall | .1 |
| port security | .2 |
| IPsec | .3 |
| IDS (Intrusion Detection System) | .4 |

ב. בעת משיכת כ�ף ממכשיר כספומט מתרכש תהליך אימות של זהות המשתמש באמצעות כרטיס האשראי והקוד הסודי שלו. מהו המונח המתאר את סוג האימות?

- | | |
|------------------------------|----|
| Single factor authentication | .1 |
| Two factor authentication | .2 |
| AAA authorization | .3 |
| AAA accounting | .4 |

ג. קבעו לגבי כל אחד מן ההיגדים שלහן אם הוא **נכון או לא נכון**, והקיימו בעיגול את התשובה הנכונה.

1. AES הוא פרוטוקול הצפנה א-סימטרי.
נכון / לא נכון
2. AES משתמש ב-**Diffie Hellman Key Exchange** כדי להצפין את המידע.
נכון / לא נכון

735913 שימושי ניתוב IP ואבטחה ברשותות קמפווס, אביב תשפ"ב, סמל

- ד. קבעו לגבי כל אחד מן ההיגדים שלහן אם הוא **נכון** או **לא נכון**, והקיפו בעיגול את התשובה הנכונה.
1. בפונקציה מסווג גיבוב (Hashing) ניתן לאחזר מהמידע המקורי את המידע המקורי. **נכון** / **לא נכון**
 2. שיטת הגיבוב SHA משתמשת ב-RSA לצורך אימות. **נכון** / **לא נכון**
- ה. מנהל האבטחה בארגון מעוניין להגביר את רמת האבטחה ב망גי החברה.
איזו מהפעולות שלහן **איןיה** תורמת להגברת האבטחה?
1. כיבוי ממשקי המותג שאינם פעילים (shutdown)
 2. הגדרת Port security על ממשקי המותג
 3. הגדרת VTY על Telnet Port 23
 4. שינוי ערך ה-native vlan ל-400
- ו. איזו מבין המתפקידות שלහן היא דוגמה ל- **Reconnaissance attack** (מתකפת סיור או איסוף מידע כללי)?
- .1 Port scan attack
 - .2 MAC address overflow attack
 - .3 DHCP starvation attack
 - .4 Man in the middle attack
- ז. קבעו לגבי כל אחד מההיגדים אם הוא **נכון** או **לא נכון**, והקיפו בעיגול את התשובה הנכונה.
1. פרוטוקול האבטחה IPsec תומך באמץאות AH באימות (Authentication) ובשלמות המידע (Data integrity).
 2. פרוטוקול האבטחה IPsec תומך באמץאות ESP רק בסודיות (Confidentiality) ובשלמות המידע (Data integrity).



שאלה 5 (20 נקודות)

ענו על חמשה מ בין השעיפים א'-ו' על-פי הנחיות שבכל סעיף (לכל סעיף – 4 נקודות).

א. התבוננו בפלט שלහן:

```
R1(config)#enable secret level 15 cisco123
R1(config)#username ADMIN privilege 15 secret Pa$$w0rd
R1(config)#aaa new-model
R1(config)#tacacs-server host 192.168.100.250 single-connection key tacacs-key
R1(config)#radius-server host 192.168.100.252 key radius-key
R1(config)#aaa authentication login default group tacacs+ enable
R1(config)#aaa authentication login CISCO group radius local enable
R1(config)#line vty 0 15
R1(config-line)#login authentication CISCO
R1(config-line)#line console 0
R1(config-line)#login authentication default
R1(config-line)#end
```

מנהל הרשת הגדר אימות על נתב R1 באמצעות פרוטוקול AAA.

לאחר מכן, הוא התחבר מרוחק לנtab באמצעות פרוטוקול Telnet.

אם שרכי האימות אינם תקינים **ויחול בהם כשל**, מה יהיה מצבם האימות או תהליך האימות לנtab R1?

1. תהליך האימות יפסיק ולא תהיה גישה לנtab R1

2. ניתן יהיה להשתמש בשם המשתמש ובסיסמה שהוגדרו במצב privilege mode

3. ניתן יהיה להשתמש בשם המשתמש ובסיסמה שהוגדרו מקומית login local על הנתב

4. ניתן יהיה להשתמש בשם המשתמש ובסיסמה שהוגדרו במצב console mode

ב. קבעו לגבי כל אחד מההינדים אם הוא **נכון** או **לא נכון**, והקיימו בעיגול את התשובה הנכונה.

1. IPS host יכול להגונן על המחשב מפני מתקפות בלתי מוכנות – zero day **נכון / לא נכון**

2. כאשר IPS מזהה איום, הוא שולח התראה למנהל הרשות בלבד. **נכון / לא נכון**



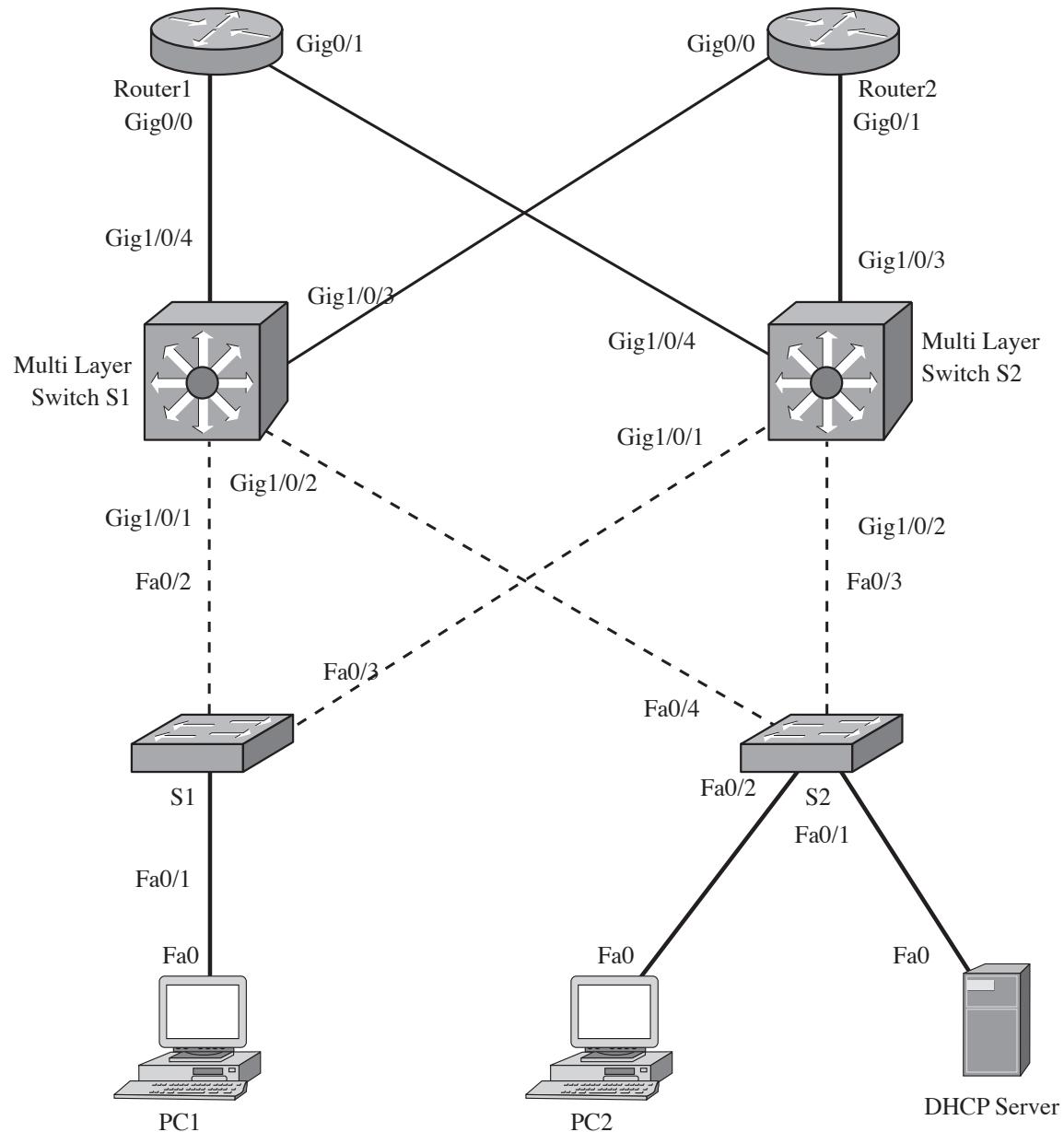
735913 יישומי ניתוב IP ו Abedha ברשותם קמפוס, אבב תשפ"ב, סמל

- ג. איזו מבחן המתאפשר שלහן ניתן למנוע עליידי נטרול של הпрוטוקולים CDP ו-LLDP על גבי התקן של חברת סיסקו?
- Brute force attack .1
 - Man in the middle attack .2
 - SYN flood attack .3
 - Reconnaissance attack .4
- ד. מנהל הרשות הגדר Port Security על מותג של חברת סיסקו. על-פי מדיניות האבטחה של החברה, אם התקן שאינו מורשה ינסה לגשת לרשות, המותג ידחה את המנה ולא ישלח הודעה עדכון על ההפרה. איזה מצב הפרה (violation mode) צריך מנהל הרשות להגדיר על ממשקי המותג?
- off .1
 - protect .2
 - shutdown .3
 - restrict .4
- ה. מנהל הרשות הגדר את ממשקי של מותג S1 למצב PortFast. איזה יתרון אבטחה מתתקבל כאשר מאפשרים BPDU guard על ממשקים אלו?
1. יכולת למנוע ממתגים שאינם מורשים להתחבר לרשות
 2. יכולת להגן מפני לולאות בשכבה 2
 3. יכולת למנוע מתקפת buffer overflow
 4. יכולת להגן מפני root bridges



יישומי ניטוב IP ובטיחה ברשותת קמפוס, אביב תשפ"ב, סמל 735913

1. התבוננו בטופולוגיה שלהן:



יישומי ניתוב IP ו Abedha בשרותים קומפוז, אביב תשפ"ב, סמל 735913

מחשבים PC1 ו-PC2 מקבלים כתובות IP משרת DHCP.

כל המחשבים והשרת מוגדרים באותו VLAN.

על כמה מבין הממשקים המוצגים בטופולוגיה יש להגדיר כחלק מהגדרת DHCP snooping trusted ports ?

- .1. על משק אחד
- .2. על שלושה ממשקים
- .3. על חמישה ממשקים
- .4. על שבעה ממשקים

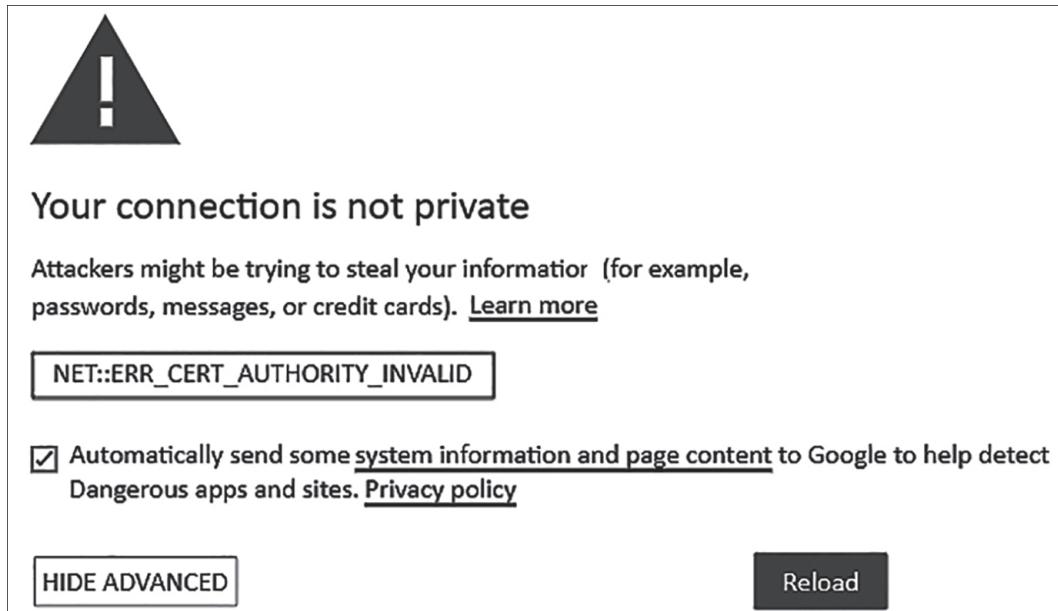
الكتاب في هذه المنطقة

ישומי ניתוב IP ובטחה ברשות Kmpos, אביב תשפ"ב, סמל 735913

שאלה 6 (20 נקודות)

ענו על חמשה מ בין הסעיפים א'-ו' על-פי הנסיבות שבכל סעיף (לכל סעיף – 4 נקודות).
שםו לב: סעיפים ה' ו-ו' תלויים זה בזאת.

א. משתמשים גלוו לאוֹרָןְטֶןְט וקיבלו את הודעה זו:



מה אינה יכולה להיות הסיבה להופעת הודעה זו?

.1. הדיקטט TLS Certificate אינה מעודכנת

.2. האתר מזוייף

.3. האתר נמצא תחת מתקפת Man in the middle

.4. האתר נמצא תחת מתקפת Brute force

ב. קבעו לגבי כל אחד מן ההיגדים שלහן אם הוא נכון או לא נכון, והקיימו בעיגול את התשובה הנכונה:

.1.ASA אפשר – כבירית המחדל שלו – תעבורת מאзор אבטחה גבוהה לאיזור אבטחה נמוך בלבד.

.2. כבירית מחדל – תידחה תעבורת מאזרים בעלי משקל אבטחה זהה, ומהנה טיפול.



735913 יישומי ניתוב IP ו Abedha ברשותות קמפו, אביב תשפ"ב, סמל

- ג. 1. מנהל הרשות הגדר את התקן ה- ASA. לפניכם חלק מן ההגדירות שהגדר המנהל. ההגדירות תקינות. על-פי הפלט שלפניכם, השלימו את מספר ה- security level שבל משקיק לקבל כבריות המודול שלו.

ASA1(config)# int gig0/0

ASA1(config-if)# nameif inside

ASA1(config-if)# exit

I. השלימו את מספר ה- :security level

ASA1(config)# int gig0/1

ASA1(config-if)# nameif outside

ASA1(config-if)# exit

II. השלימו את מספר ה- :security level

ASA1(config)# int gig0/2

ASA1(config-if)# nameif data-center

ASA1(config-if)# exit

III. השלימו את מספר ה- :security level

2. מנהל הרשות רוצה לשנות את מספר ה- security level של int gig0/2 ל- 20 . איזו פקודה עליו להקליד לשם כך? כתבו את הפקודה במקום המתאים.

ASA1(config)# int gig0/2

ASA1(config-if)# _____

ASA1(config-if)# Exit

الكتاب في هذه المنطقة

لذلك يجب أن يكون هنا



نزع ورقة قد يؤدي إلى إلغاء الامتحان

735913 יישומי ניתוב IP וابتחה בראשות Kmpos, אביב תשפ"ב, סמל

ד. לפניכם לכידת תעבורות (capture traffic) רשות.

המשך בעמוד 23 ◀



735913 יישומי ניתוב IP ובטיחה ברשותן למינוס, אביב תשפ"ב, סמל

כיצד היה ניתן למנוע את החולשה המוצגת בהקלטה זו?

1. באמצעות שימוש ב프וטוקול SSH

2. באמצעות שימוש בפרוטוקול Telnet

3. באמצעות שימוש ב-IPS

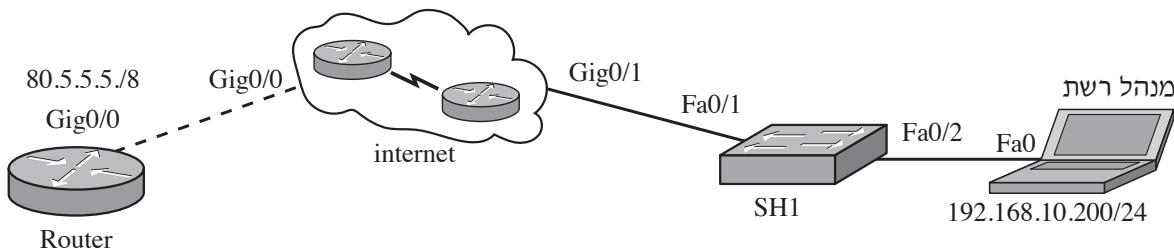
4. באמצעות enable secret

الكتاب في هذه المنطقة

لذلك يجب أن يكون في هذه المنطقة

735913
ישומי ניתוב IP ואבטחה ברשות Kmpos, אביב תשפ"ב, סמל 13

הטופולוגיה והפלט שלהן מתיחסים לסעיפים ה' ו-ו', התלוים זה זהה.



```

Router#show ip access-lists
Extended IP access list SEC-ACL
  5 deny ip any host 80.5.5.5
  10 permit tcp host 192.168.10.200 host 80.5.5.5 eq 22
  
```

ה. מנהל הרשות אינו מצליח להתחבר לנטב router **בצורה מאובטחת**. מה הבעיה?

1. רשימת הגישה אינה מאפשרת גישה ב프וטוקול Telnet
2. כתובת ה-IP של הנטב אינה חוקית
3. רשימת הגישה חוסמת את כל המשתמשים מLAGEST לנטב
4. לא הוגדרה רשימת גישה סטנדרטית

ו. כיצד ניתן לאפשר גישה מאובטחת אל הנטב ממוחשבו של מנהל הרשות בלבד?

תשובה:

בהתלהה!



טיוויטה

←
لُكْسْبِنْ في هذه المنطقة

لَا يَأْتِي ثُوبَ الْأَزْوَارِ إِلَّا مَعَهُ



ישומי ניטוב IP ואבטחה ברשות קמפווס, אביב תשפ"ב, סמל 735913

טיוויטה



טיוויטה

←
لُكْسْبِنْ في هذه المنطقة

لُكْسْبِنْ في هذه المنطقة

מذבקת משגיח

ملصقة מראقب

"**איתיך בכל מקום, גם בבוגרות.**

בהצלחה, מועצת התלמידים והנווער הארץית"

"**معك في كل مكان، وفي البحروت أيضًا.**

"بالنجاح، مجلس الطلاب والشبيبة القطري"

נספח: מילון מונחים (2 עמודים)

לשאלון 735913, אביב תשפ"ב

המונה	תרגם המונח		
	אנגלית	רוסית	ערבית
פרק ראשון – יישומי ניתוב IP			
אימות	authentication	Идентификация	التحقق
גיבוי	backup	Резервная копия	الحفظ الاحتياطي
המרה	conversion	Преобразование	تحويل
טבלת טופולוגיה	topology table	Таблица топологии	جدول طوبولوجيا
טבלת ניתוב	routing table	Таблица маршрутизации	جدول توجيه
טבלת שכנים	neighbors table	Таблица соседних элементов	جدول جيران
ולאות ניתוב	routing loops	Петли маршрутизации	حلقات التوجيه
מארח	host	Хост-компьютер	مضيف
منה	packet	Пакет	وجبة (دفعة)
מצב קישור	link state	Гиперссылка	حالة الارتباط
נתיב	path	Путь	مسار
שרת	server	Сервер	الخادم

פרק שני – אבטחה ברשותן קמפוס

אלגוריתם	خوارزمية	خوارزمية	خوارزمية
הצפנה	Шифрование	تشифير	تشифير
חיבור טרמינל	Подключение терминала	محطة اتصال	محطة اتصال
MUX	Интерфейс	واجهة	واجهة
RSA מפתח	RSA-ключ	RSA	RSA
ΜΑΤΓ	Коммутатор/ Переключатель	مفتاح	مفتاح
נמען	Получатель	مستلم	مستلم
נתב	Маршрутизатор	راوتر	راوتر
פורט	Порт	منفذ	منفذ

תרגום המונח			המונח
אנגלית	רוסית	ערבית	
protocol	Протокол	بروتوكول	פרוטוקול
access list	Список доступа	قائمة الوصول	רשימת גישה
network	Сеть	شبكة	רשת
configuration	Конфигурация	مواصفات	תצורה